Security System of Logistics Service Transaction Record Based on Wireless Network

Yanhong Su and Lijing Yu
School of Business, Yantai Nanshan University, Yantai, Shandong 265713, China

Correspondence should be addressed to Yanhong Su; 2016150198@jou.edu.cn

Received 24 May 2022; Revised 11 July 2022; Accepted 18 July 2022; Published 1 September 2022

Copyright © 2022 Yanhong Su and Lijing Yu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless Networks (WNs) and their associated technology paradigms are employed for smart and secure logistics services. The wireless logistics transactions are secured through end-to-end authentication, verification, and third-party watchdog systems. This manuscript introduces a Preemptive Security Scheme for Transaction Verification (PSS-TV) in wireless network-aided logistics services. Different logistics services are secured based on the sender and receiver’s signature in mutual consent. Signature generation and implications are varied using the key size and validity based on the previous transaction recommendation. The conventional random forest classifier learning is used for detecting transaction breaches and validity requirements. This is feasible based on the transaction interruptions and failed mutual verifications. These classifications are performed using the learning paradigm for improving the key size in generating stealthy signatures. In the signature generation, the conventional elliptic curve cryptography is relied upon. The proposed scheme’s performance is analyzed using success ratio, failure rate, verification and authentication time, and complexity.

1. Introduction

A wireless network operates using radio frequency (RF) signals that provide connection among the nodes in the network. The wireless network is widely used in various fields, such as home appliances, business places, wearable devices, and telecommunication processes [1]. Logistics operations are a process that moves the goods or products from the manufacturer to the consumers. Logistics operations provide the entire process of products and produces necessary data for a management system [2]. The operations, such as planning, labeling, transport, production details, and packaging of products, are identified and analyzed. Logistics operations use wireless networks to provide appropriate services for consumers. Delivery time, product detail, supply mode, and product cost details are produced by logistics operation [3]. Wireless networks are mostly used for transaction and management processes that provide accurate details about manufacturers to the customers. A global positioning system (GPS) is done by using a wireless network. GPS provides necessary details about goods for the customers that enhance the performance of the logistic operation. GPS sends information for the logistic operation that contains the actual details about the goods [4, 5].

A wireless logistic system is a network that organizes people, products, resources, information, activities, and organizations to provide proper supply to the customers. Product handling, order processing, packaging, transportation, and warehousing are some of the processes that occur in the wireless logistics system [6]. Wireless logistics system has various security and privacy issues that cause major problems in providing services for customers. Risks such as data locality, third-party risks, fraud, and data protection are some of the traction problems that are available in the wireless logistics system [7]. Transaction security is used in wireless networks and systems that ensure users’ safety from third-party members. Transaction security framework contains details, such as interaction, services, notification, and actions over products with a certain set of policies and rules [8]. Transaction security provides various
privacy and security policies for the users that protect the clients from hackers. The supply chain security method is used in wireless logistics system that provides necessary services for the users. The supply chain method identifies the risk and problems in the logistic system and provides optimal solutions to solve the problems [9, 10].

A secure transaction process is a complicated task to perform in a logistics system that ensures the safety and security of customers from third-party members. The logistic system provides services, such as production, distribution, supply, and reverse operations [11]. Various methods are used in ensuring the transaction process in the logistic system. Records-based transaction process is mostly used to improve the security measures in the logistics system. Records such as stock records, consumption records, and transaction records are the records that are included in the logistic system [12, 13]. Transportation details, packaging details, order details, and product details are recorded in the logistic system. Record-based transaction method transfers the goods and products from manufacturers to the consumers [13]. Record-based transaction method improves the overall security services for the consumers and reduces the risk rate in the transaction process. Transaction details are protected and prevented from attackers, which improves the trustworthiness among the consumers in the logistic system [14]. Blockchain-based transaction method is also used in the logistic system that provides a secure transaction process for the users. Wireless sensors are used in blockchain to find out the attackers and provide optimal solutions to solve the attacks [15].

2. Related Works

Toorajipour et al. [16] introduced a blockchain-based business transaction model for international trades. The proposed model is used to identify third-party members during transactions in international trade. The blockchain technology-based letter of credit (BTLC) mechanism is used in the proposed model to analyze the standards and activities in the transaction process. The proposed model reduces the problem rate in the transaction and ensures consumer security from attackers.

Chen et al. [17] proposed an intelligent antiswitch package method using a blockchain approach for a logistic system. The proposed method is used to find out the location and condition of packages that are needed to be delivered. A global positioning system (GPS) is used here to trace the location of the package. The blockchain approach collects necessary information from the organization and provides solutions to solve the problems in the package tracing process. The proposed method improves the accuracy rate in the tracing process, which increases the efficiency of the logistic system.

Liu et al. [18] introduced a new blockchain-based data privacy protection method for logistic systems. The main goal of the proposed method is to prevent the user's transaction data from third-party members. A private key is shared among users for access control policies that ensure the privacy of users from attackers. The blockchain approach compares the private key with recorded data and provides access to the users. The proposed privacy protection method improves the feasibility and reliability of e-commerce logistic systems.

Fu et al. [19] introduced a hyperconnected trunk logistics alliance (HTLA) framework for logistics systems. Both big data analytics and blockchain mechanism are used in the HTLA framework. Big data analytics collects logistics information, such as product details, shareholders, and transaction details of consumers. HTLA framework increases the trustworthiness among the consumers that reduces the negative rate in the logistics system. The proposed method is a privacy protection control framework that improves the security level of users in the transaction process.

Savic et al. [20] proposed an anomaly detection (AD) method using the deep learning (DL) technique for cellular Internet of Things- (IoT-) based logistics devices. IoT is mostly used in logistics devices to provide many services for users. Autoencoders are used in AD to find out the risks and problems in logistics devices. AD method identifies the anomalies that are presented in devices and provide optimal solutions to solve the problems. The proposed AD method improves the accuracy rate in the detection process, which increases the efficiency of the devices.

Tesei et al. [21] introduced a distributed ledger technology- (DLT-) based credential management system for logistic vehicles. The proposed method is a security scheme for the logistics vehicle tracking process. DLT is used here to enable a transparent tracking process for logistic vehicles. Services such as allocation, authorization, authentication, and revocation are produced by the proposed method that improves the feasibility of the system. The proposed DLT method increases the effectiveness and efficiency rate of the system.

Ruesch et al. [22] proposed a positive planning scheme for ensuring logistics facilities in urban places. The main aspect of the proposed scheme is to identify the locations and positions of urban areas. Certain strategies are performed here to fetch the necessary details for a positive planning process. The proposed scheme increases the performance and development rate in urban areas. The proposed scheme improves the feasibility and reliability of logistic facilities in urban areas.

Zhan et al. [23] introduced an Internet of Everything- (IoE-) based smart logistic network (IoE-SLN) for the logistic system. The proposed method is mainly used to improve the optimization process. IoW-SLN also provides various services for the communication process among consumers and manufacturers. Both computation cost and energy consumption rate in the computation process is reduced. The proposed IoE-SLN improves the accuracy rate in Quality of Services (QoS) that provide necessary services to the users.

Zhang and Jin [24] proposed a neural network- (NN-) based credit system for smart logistics public information platforms. Machine learning algorithms are used here to improve the efficiency of the NN system. The proposed credit system is an analysis process that analyzes the credit ratings of
enterprises and shareholders. NN provides necessary information for the transaction process that reduces the latency rate in the analysis process. The proposed system improves the performance and effectiveness of smart logistics.

Li et al. [25] introduced a blockchain-based privacy-preserving storage scheme for logistics data. A cloud server is used here to store the logistic data and an aggregation method is used to encrypt the data from the server. The blockchain approach is used here to improve the privacy and security of users’ data from third-party members. Experimental results show that the proposed privacy-preserving scheme improves the performance and reliability of the system.

Sun et al. [26] proposed a blockchain data query algorithm using searchable encryption for logistics information. Logistics information is divided into various data files and encrypted using searchable encryption. Data files are encrypted with a certain keyword index value that improves the privacy of users from attackers. Keyword index values are stored in the blockchain to fetch necessary data for the analysis process. The proposed method improves the feasibility and effectiveness of logistics information.

Zhang et al. [27] introduced an improved genetic algorithm for the seeker optimization process. The proposed algorithm is mostly used to find out the behaviors of logistic vehicles and produce an optimal set of data for the optimization process. The proposed method is used to solve the cold chain logistics vehicle’s problem and improves the optimization process. When compared with other algorithms, the proposed algorithm reduces the computation cost, which improves the efficiency of the system.

3. Proposed Scheme

The design goal of the PSS-TV method is to improve end-to-end security in wireless logistics transactions by reducing interruptions and failures based on the transaction through conventional elliptic curve cryptography. This platform provides authentication, verification, secure transactions, and third-party watchdog systems for a wide range of WNs assisted smart and secure logistic services. It experiences providing authentication to the logistic services through the sender and receiver’s signature in mutual consent. It requires a security signature that is to be generating a key for secure and authenticable logistic transaction services through wireless logistic services between the sender and receiver. The operations of logistic services and transaction security through wireless network platforms are used for providing authentication, verification, and transaction security. The process of signature generation is differed using key size variations and key validity based on the previous recommendations is analyzed using learning (as shown in Figure 1).

This signature authentication method is provided for transaction security through the wireless network and functions of the logistics services. In this proposed work, random forest classifier learning is used to detect transaction breaches and validity requirements are performed based on the previous transaction recommendation. The learning process is to improve the key size in generating stealthy signatures required transaction security based on wireless network-assisted logistics transactions inputs. The transaction inputs are required from the logistics services based on the signature generation and implications in the logistic service transactions at regular time intervals. This scheme aims to reduce the failure rate, complexity, and interrupt ratio observed in logistics services. The challenging role is the maximization of key size and validity with the previous transaction recommendation.

3.1. Logistics Service Transaction Based on Signature Generation Process. The wireless logistics transaction is determined using two types of services, namely, the sender and receiver information. The logistics services are responsible for a large amount of product delivery and transaction fee, fleet and shipping address administering security, and other mitigating previous transaction recommendation. The logistics services communicate with $L_S = \{1, 2, \ldots, s\}$ set of logistics services that are capable of processing transactions from all the senders and receivers in the smart technology. The above $L_S$ transacts different types of product delivery at any time interval $T_R = \{1, 2, \ldots, t\}$. Let $N$ denote the number of logistics services that are presently pursued in wireless logistics transactions. Based on the above representation, let the number of logistics services per unit time be $i$ such that the different function based on the transactions $F_i$ is computed as

$$F_i = \begin{cases} \frac{L_S + i}{t} \forall L_S \rightarrow T_R, & \text{if } N = 0, \\ L_{T_S} \times \frac{s - N}{L_S} \forall (L_S, n) \rightarrow T_R, & \text{else } N \neq 0. \end{cases}$$

such that
In equation (1), the variable \( L_{T_L} \) denotes the logistics transactions and signature generation in \( T_R \). In the above condition, \( L_S \rightarrow T_R \) and \( (L_S, m) \rightarrow T_R \) analyze the shipping address, fee, and delivery on wireless networks and the secure logistics services in the various time instances \( T_R \). The authentication of the sender service or information from the transactions process is analyzed in two levels, namely, authentication and verification based on the sender and receiver services, and \( F_i \) are the additional factors for securing the transactions depending on whether the logistics services \( T_R \) is satisfied. For wireless logistics transactions, the sender provides some services based on transaction recommendation and secure authentication for the sender services. The authentication of services from the sender side \( L_S \in i \) and \( N \) function through the wireless network of their records and transactions time. From the above equations (1) and (2), the constraint \( N > L_S \) specifies less and insufficient logistics services in the transactions. The various time instances for the logistics services and the consecutive process \( F_i \) rely upon \((s \times i)\), which is the computation of transaction service authentication.

\[
 L_S \rightarrow T_R = \prod_{i=1}^{l_n} l_N * st. \quad (2)
\]

\( \neg F_i = \frac{F_i}{(i+N)} - (F - L_{T_R}). \quad (3)\)

Based on the above condition, the variables \( T_R \) and \( \neg F_i \) represent the different logistic services at any time interval and series of transaction services. The above equation is the reliable process of providing the signature generation \((S_g)\), which is computed for each stage of \( T_R \). This assessment is processed for identifying the services based on the conditions \( N \neq 0 \) and \( N = 0 \) for all \( T_R \) using the conventional elliptic curve cryptography method for secure transactions. This elliptic curve cryptography method is an approach to provide security and it relies on elliptic curves at each stage in that wireless network. The different secure logistics service instances of \( S_g, T_R \) and \( \neg F_i \) such that the signature generation is determined for all the sender service output for authentication \( A_u \). Figure 2 presents the service authentication process for different \( F_i \).

The different transaction data is extracted from \( L_S \) for \( \neg F_i \), \( \neg F_i \) is split into interval-based authentication based on \( S \) and \( \Delta s \), which are discussed below. The generating function is responsible for \( S^g \neg F_i \); that is split into \( F_i \in L_S \). \( \exists T_R \) is required for preventing high complexities for maximizing the secured transaction (Figure 2). The solution for transaction security of \( \neg F_i \) in \( T_N \) is the mutual consent signature for augmenting the logistics services \((s \times i)\). The authentication is based on the sender service and the final output \( \exists \) is detected from the transaction service in defining \( S_g \). The different instances of transaction inputs for the representation of \( \neg F_i \) for both the condition \( L_S \rightarrow T_R \) and \( (L_S, N) \rightarrow T_R \) that includes different logistics services if the transaction is analyzed in a different time interval. The output of the signature generation in the sender service \( L_S \rightarrow T_R \) solves secured transactions, whereas \( (L_S, N) \)
--- $T_R$ extracts outputs of $s$ with $N \neq 0$. The equation indicates the signature generation and implication and the final output of $\exists$ the condition $(L_S, N) \rightarrow T_R$ is assessed. These assessments are performed for both the sender and receiver sides based on the condition of $L_{T_R}$ and the computation of $N = 1$ or $N = 0$ in $T_R$. Hence, the solution is analyzed for the different logistics service instance $T_R$. As per the above condition, $N$ serves as transactions input and the authentication of $L_{T_R} \in L_S \rightarrow T_R$ is computed as

$$A'_s = \neg F_i T_R - L_{T_R} + \exists N. \quad (4)$$

Instead,

$$\exists F_s = \neg F_i T_R - L_{T_R} + \exists N_i. \quad (5)$$

Equations (4) and (5) represent the signature generation output for each stage of logistics service transactions. It is determined as $\neg F_i T_R - L_{T_R} + \exists N_i$ based on $N = 0$; then, $N = 1$ and $\neg F_i T_R = N \exists_i$, and therefore, $Z = N T_R t + \exists N_i = N \exists_i (t + 1)$ is the precise result and $S'_g = 1$. Here, the authentication of such sender-side service and information is retained. The secure transaction requires authentication, verification, and third-party watchdog systems for each stage of the processing $T_R$ and this logistics service provides security signatures based on mutual consent. Therefore, $(L_S, N) \rightarrow T_R$ the service output and final solution are computed as in the above equation, respectively.

This consecutive process is not relevant for the first assessment as in the above-derived equations (5) and (6); here it depends on transactions services $L_S$ to the $T_R$. Therefore, $S'_g$ and implications together with $\exists$ and $L_S$ is analyzed and provides security by the wireless network and hence it remains ideal. The consecutive instance of logistics transactions services, based on $S'_g$ with the previous transaction recommendation $D_T$, defines the stealthy signature distribution of available services. In this process, the sequential logistics transactions are analyzed in $N > i$; then, the transaction breaches and validity requirements are observed through a conventional random forest classifier based on the condition $s \in L_S$ being halted to prevent transaction interruptions and failed mutual verifications from both sender and receiver services in the wireless network, relying on previous transaction recommendations and verification processes on the receiver side. The security distributions in the logistics transaction services information are shared through wireless networks with the end-to-end verifiable security key to their receiver service in $T_R$. The classifier process for failure and validity is presented in Figure 3.

$F_i$ is verified for validity and failure based on $i = 1$ to $s$ and $T_R$; then, classification is required for preventing interruptions. The classifications are either recurrent or nonrecurrent based on $Z$ and $\exists$, respectively. In the alternating sequences, $\exists F_s$ is validated for preventing failures such that the reassignment requires authentication $\forall S \in L_S$ (refer to Figure 3). This consecutive manner of providing authentication and verification on both sender and receiver services overcomes transaction interruptions and failed mutual verifications by processing unwanted/incorrect shipping address or delivery in transactions increasing failure rate and complexity. At the same time, the success ratio and verification are high. The secured transactions make certain authentication services delay and mutual verification within the transactions. In the record storing process, the logistics transactions service follows the signature for entering into the network. The mutual consent depends on $(\exists, S'_g, L_S)$ for verifying the sender and receiver is already in that network or new to the network is identified with mutual verification. This mutual verification requires some authentication for users’ information being administering based on the previous transactions’ recommendation and $S'_g$ simultaneously. In this transaction security process, the end-to-end authentication and verification keys are distributed between the sender and receiver services; using elliptic curve cryptography, the following are steps to generate an end-to-end key.

**Step 1.** Select any two large prime numbers $U$ and $V$ such that $U \neq V$, based on sender and receiver services.

**Step 2.** Estimate

$$s = U V. \quad (6)$$

**Step 3.** Estimate the function

![Figure 2: Service authentication process.](image-url)
\[ \Delta(s) = (U - 1)(V - 1). \]  \hspace{1cm} (7)

**Step 4.** Select an integer \( x \) such that \( L_S < x < \emptyset(s) \), which is relatively prime to \( \emptyset(s) \).

**Step 5.** Compute signature \( S_g \) such that
\[ S_g x \equiv 1 \pmod{\Delta(s)}. \]  \hspace{1cm} (8)

The security key consists of the \( s \), the signature generation, and the variable \( x \) represents the public exponent for sometimes performing encryption service, whereas the private key consists of \( s \), the signature generation, and \( x \) for the private exponent and sometimes performing decryption service, which can be hidden. The logistics transacts services from sender to receiver; it provides the private key for secret records. The variables \( U \) and \( V \) are exposed since the factors of \( s \) allow the signature of \( S_g \) based on \( x \). This key process provides signatures and implications based on the sender and receiver services. The services are modified using the key size and validity of the key based on the previous logistics transactions recommendation. The end-to-end authentication process between the sender and receiver is depicted in Figure 4.

The authentication and verification processes are balanced between sender and receiver \( \forall F_\ell \in \overline{F}_{i \ell} \). The failure check is based on \( S_g x \Delta 1 \) validation from the receiver end. In this validation process, the \( \exists T_R \approx \Delta(s) \) is the alternating verification after \( (\exists, S_g, L_s) \) assignment \( \forall i > 1 \) to \( s \). Contrarily, \( (F_{i \ell}, s) \) is required for \( i > 1 \) based on \( \Delta(s) \) such that verification is performed (refer to Figure 4). The logistics services are performed based on the end-to-end authentication and verification of all the transaction services or previous transaction recommendations \( T_R \). The classification process is performed, along with \( \exists V_i, T_R \) being required. Therefore, the wireless network processes all the levels of services and maintains the records for future verifications of logistics transactions service, handling the set of transaction functions, where the first instance \( L_S \) denotes the logistics service for \( T_R \) and the next denotes the receiver side services.

It is to be accounted for the authentication and verification modification, forwarded under \( T_R \) or \( S_g \) and it is analyzed in the records. In the records, each level service with serving logistics inputs is aided for the following computation for further process. In this condition, the complexity is estimated as follows:
\[ C = \frac{T_R(\ln N)}{F(M_V)}. \]  \hspace{1cm} (9)

In equation (9), the variables \( \ln N \) and \( M_V \) denote the occurrence of transaction interruptions and failed mutual verification as classified in the conventional forest classifier learning. This complexity is validated for the next sequential instance with the detection of transaction breaches and validity requirements. Therefore, if \( C = 0 \), then the following next instance if \( s[N(T_R)] = 0 \) is classified under the learning process. Similarly, if \( L_S > T_R \), then \( C = 0 \) and therefore, the classification process of \( C = 0 \), which means the signature generation and implications are observed in the logistics services. This detection of signature is valid until the above constraint fails. The incorrect shipping address and delivery provided are detected for analyzing the complexity of that wireless network. This process is aided for classification and the breach and key validity detection process is performed based on the modifications in the records.

The identification of stealthy signature is addressed in the transactions from sender to receiver services or vice versa in the conventional process. Therefore, there are some least possible occurrence of transaction breaches that is misguided as failures in the network; the above transaction interruptions and failed mutual verification detected from the classification process based on end-to-end authentication and verification on both sender and receiver services improve the key size and validity to reduce the complexity and failure rates in different intervals. In Figure 5, recommendation (%) and key size analysis under varying \( s \) are analyzed.

Figure 5 presents the analysis of recommendation (%) and key size for the varying \( s \). As \( s \) increases, the transactions are high for verification and validation. The classifier learning identifies \( \exists \) and \( Z \) for preventing failures. As the failure reduces, the recommendation increases. On the contrary process, \( (\exists, S_g, L_s) \) the validations for \( i = 1 \) to \( s \) are performed wherein \( \exists T_R \equiv \Delta(s) \) is verified. Therefore, in this process, the key size is varied for strengthening the authentication. The proposed scheme identifies different intervals for providing stealthy authentication. Therefore, \( \exists T_R \) is performed such that \( E_{x} \) is induced for improving verification checks. This achieves a high key size for sustaining
security under varying session intervals. An analysis of complexity over the varying $T_R$ (%) is presented in Figure 6.

An analysis of complexity over the varying $T_R$ (%) is presented in Figure 6. Based on the recommendation, the complexity varies and hence the verification is induced. Depending on the interference (session) and key validity, the complexity is analyzed. For confining the $L_S$ validations for $S_g \Delta 1$, the new $\Delta (s)$ generates novel verification instances. These instances are used for providing less complex authentication under controlled failures. The analysis for verification time for different instances is presented in Figure 7.

The verification time varies with the transactions and for which the key size varies; hence, authentication and validation are required. As the key size increases, the validation requires $\exists S_g, L_s$ or $\exists T_r$ based verification. This verification is concurrent for failed (interrupted) and independent for new authentication. Therefore, the verification time is high for the classified instances, improving the transactions.

![Figure 4: End-to-end authentication between the sender and the receiver.](image)

![Figure 5: Key size and recommendation analysis.](image)

![Figure 6: Complexity for varying $T_R$ (%).](image)
4. Discussion

This section discusses the proposed scheme’s performance using experimental data analysis. The data from [28] is shared between two logistics information systems by employing ECC encryption. This data set contains 5000+ records with 6 fields including freight time and charges. The information is supposed to be stored in the database after the decryption process and hence the transactions are varied between 200 and 100 for a maximum validity of 80 min. With this information, the metrics success ratio, failure ratio, authentication time, verification time, and complexity are analyzed. In the comparative analysis section, the existing HTLA [19], DL-AD [20], and B-SSS [25] are considered.

4.1. Success Ratio. According to Figure 8, wireless networks and their related technologies are used for smart and secure logistics services, providing security-based end-to-end authentication and wireless logistics transactions. The third-party system will provide the same logistics service through a sorting process, relying on the signatures of the sender and receiver for mutual verification. The detection of transaction interruptions and failed mutual verifications are classified and signature generation from the first stage outputs in signature authentication enhances the success ratio and security for the logistics services wherein the security of the transactions based on the conventional elliptic curve cryptography can be used for generating the signature. This problem is addressed using transaction breaches that can be analyzed for satisfying successive signature authentication based on the logistics services depending on the interruptions, preventing failed mutual verifications. Therefore, the logistics transaction services based on the authentication and verification in both sender and receiver services are detected, preventing a high success ratio until new signature generation.

4.2. Failure Ratio. Secure logistics services vary based on key size and validity. The signatures based on previous transaction recommendations and based on the mutual agreement of the sender and receiver in different situations are shown in Figure 9. In these different logistics services, the transaction breaches and validity requirements detection based on time intervals, such that \( L_S \rightarrow T_R \) and \( (L_S, m) \rightarrow T_R \), the stealthy signature, occur due to improving key size in the learning paradigm. The transactions analysis is based on service authentication of different logistics input observations, the failures and interruptions are detected in both sender and receiver end information and services are stored as records for future recommendation and verifications wherein the different logistics services with the precise key generated based on the verification modification is analyzed. In this proposed transaction verification, the signature authentication is mitigated by detecting interrupts through a random forest classifier learning process based on both sender and receiver services, is analyzed for further transactions, and is considered for providing additional logistics services for the products and good transactions. Therefore, the failure ratio is less compared to the other factors in the wireless network-based logistic transaction services, and the failure is detected.

\[
\text{Transactions } = 400, \quad \text{Transactions } = 600, \quad \text{Transactions } = 800, \quad \text{Transactions } = 200
\]

\[
\begin{align*}
\text{Verification Time (ms)} & \quad \text{Transactions } = 200 \\
& \quad \text{Transactions } = 400 \\
& \quad \text{Transactions } = 600 \\
& \quad \text{Transactions } = 800
\end{align*}
\]

**Figure 7:** Verification time for varying instances.

4.3. Authentication Time. This proposed wireless network satisfies less authentication time compared to the other factors based on transaction interruptions and failed mutual verifications detected in Figure 10. The transaction breaches and validity requirements with the previous transactions recommendation in the real-time stealthy signature detection are less for the proposed network. This is addressed by the learning process; records for distinguished services are exploited through random forest classifier learning. The interruption and failure detection and less complexity factor of smart and secure logistics services determine the authentication time under key size and validity observation based on signature in mutual verifications. The condition of \( \forall F_i = F_i / (i + N) - (F - L_T) \) whether failure detection makes a sure stealthy signature in logistics services is retained using conventional elliptic curve cryptography presented in the signature key generation process, as in equation (6). Thus, the proposed work detects the interruptions and failures based on authentication time are less.

4.4. Verification Time. The different logistics services support through transactions and previous recommendation analysis for failures are presented in Figure 11. The proposed work achieves less verification time for transactions recommendation by computing \( L_S \rightarrow T_R \) and \( (L_S, m) \rightarrow T_R \). In the different proposed security systems, logistics service transactions are analyzed based on random forest classifier learning based on the previous transactions recommendation analysis for providing signature generation and implications; these processes are analyzed depending on the condition \( N > L_s \) user verified signature at the receiver end wherein the different transactions based on logistics services preceded.
Figure 8: Success ratio analysis.

Figure 9: Failure ratio analysis.

Figure 10: Authentication time analysis.
using equation (5) computation. In this wireless network, the processing of authentication and verification $S_g$ is computed for verification timeless signature mutual verification and authentication. This unnecessary delay in authentication or verifications instant is the consideration of processing transactions recommendation and its mutual verifications based on signature (as in equation (7)). The elliptic curve cryptography method analysis for secure logistics services such that the output is alone authenticated using a generated key size and validity of the signature in mutual consent. Based on this signature, the verification time is computed for transaction recommendation and classification process.

4.5. Complexity. This proposed logistics service transactions through authentication, verification, and third-party watchdog systems are processed at any time interval based on complexity and transaction interruptions of generating a key for transaction services depending on previous transaction recommendations. The two consecutive services for both sender and receiver side provide mutual verification and authentication through random forest classifier learning. The assessment of transaction interruptions and failed mutual verification detection based on the different logistics services provides signature generation condition $\widetilde{\mathcal{F}} = L_{T_2} + \exists_{n_i},$ and then $\widetilde{\mathcal{F}}$ is computed using a stealthy signature for the first failure occurrence for the consecutive process of transaction breaches detected based on mutual verification and authentication can be processed for both conditions using the learning process. The end-to-end authentication and verification are analyzed based on signature in mutual consent at a different time interval and complexity. The proposed logistics services of transactions through random forest classifier learning depend on transaction security for which the mutual verification from their associated technology achieves less complexity as presented in Figure 12. In Tables 1 and 2, the above comparative analysis is summarized.
Table 1: Comparative analysis summary for transactions.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>HTLA</th>
<th>DL-AD</th>
<th>B-SSS</th>
<th>PSS-TV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success ratio</td>
<td>80.45</td>
<td>83.41</td>
<td>90.34</td>
<td>93.713</td>
</tr>
<tr>
<td>Failure ratio</td>
<td>20.03</td>
<td>18.29</td>
<td>15.75</td>
<td>12.288</td>
</tr>
<tr>
<td>Authentication time (ms)</td>
<td>3541.7</td>
<td>2961.8</td>
<td>2116.8</td>
<td>1258.26</td>
</tr>
<tr>
<td>Verification time (ms)</td>
<td>4265.04</td>
<td>3017.1</td>
<td>2156.7</td>
<td>1222.48</td>
</tr>
<tr>
<td>Complexity (mb)</td>
<td>625.75</td>
<td>501.83</td>
<td>354.65</td>
<td>226.861</td>
</tr>
</tbody>
</table>

Inference: The proposed scheme achieves an 8.98% high success ratio, 11.47% less failure ratio, 9.37% less authentication time, 10.18% less verification time, and 9.01% less complexity.

Table 2: Comparative analysis summary for validity.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>HTLA</th>
<th>DL-AD</th>
<th>B-SSS</th>
<th>PSS-TV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success ratio</td>
<td>80.18</td>
<td>83.55</td>
<td>89.08</td>
<td>94.53</td>
</tr>
<tr>
<td>Failure ratio</td>
<td>19.58</td>
<td>17.9</td>
<td>14.91</td>
<td>11.157</td>
</tr>
<tr>
<td>Authentication time (ms)</td>
<td>3546.4</td>
<td>2961.3</td>
<td>2089.9</td>
<td>1243.07</td>
</tr>
<tr>
<td>Verification time (ms)</td>
<td>4230.9</td>
<td>2980.1</td>
<td>2138.5</td>
<td>1270.27</td>
</tr>
<tr>
<td>Complexity (mb)</td>
<td>633.91</td>
<td>516.78</td>
<td>404.25</td>
<td>236.867</td>
</tr>
</tbody>
</table>

Inference: The proposed scheme achieves a 10.26% high success ratio, 12.61% less failure ratio, 9.39% less authentication time, 9.87% less verification time, and 9.05% less complexity.

5. Conclusion

Logistics transactions require prominent security measures for administering integrity between the sender and receiver over varying freight data. For ensuring integral authentication, a preemptive security scheme for transaction verification is presented in this manuscript. This scheme relies on conventional elliptic curve cryptography for signature generation, authentication, and verification process. The signature implication and verification levels are determined based on key validity and transaction success as classified by random forest learning. In this learning, the previous transaction and validity are analyzed for mutual verification between the sender and the receiver. Based on the interruption observed in the transaction, the security level and authentication are determined. Therefore, the classifier performs independent and concurrent verification for authenticating the transaction information shared across the connecting wireless networks. From the experimental analysis, for the varying transaction, the proposed scheme achieves an 8.98% high success ratio, 11.47% less failure ratio, 9.37% less authentication time, 10.18% less verification time, and 9.01% less complexity.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

References


